Unified Networks für das mobile Zeitalter

Bereitstellen eines skalierbaren, leistungsstarken und intelligenten Netzwerks

Inhaltsverzeichnis

Einführung

Das Verlangen nach mobiler Kommunikation war noch nie so groß wie heute. Ein Ergebnis daraus ist das BYOD-Phänomen (Bring Your Own Device). Es beruht auf der Vorliebe der Benutzer, ihre eigenen Smartphones und Tablets auch im Geschäftsleben einzusetzen. Dieser Trend veranlasst IT-Abteilungen dazu, ihre Investitionen in WLAN-Technologien (Wireless LAN) aufzustocken. Damit versuchen Unternehmen, ihren mobilen Mitarbeitern die Nutzung von Geschäftsanwendungen ohne Medienbrüche zu ermöglichen. Geschäftsanwendungen können so jederzeit, überall und mit jedem Gerät, benutzerfreundlich verwendet werden.

Das Unternehmens-WLAN wird so zum Netzwerk erster Wahl für Mitarbeiter und Vertriebspartner. Neben klassischen Anwendungen muss es auch eine zunehmende Anzahl von Echtzeitanwendungen unterstützen, z. B. für die Sprach- und Videokommunikation. Bei der Entwicklung der WLAN-Technologien wurden die Unternehmensanforderungen hinsichtlich Leistung, Skalierbarkeit, konsolidierter Verwaltung, verbesserter Gesamtbetriebskosten und vor allem hinsichtlich Sicherheit noch nicht berücksichtigt. Neben der Belastung des WLAN durch den Einsatz von Echtzeitanwendungen zwingt die massive Zunahme mobiler persönlicher Geräte die Unternehmen dazu, ihren Geschäftsbetrieb, ihr geistiges Eigentum und ihre vertraulichen Informationen stärker zu schützen.

Wie also sollte ein Unternehmen den Erwartungen ihrer mobilen Mitarbeiter gerecht werden? Die Lösung ist ein intelligentes, einheitliches und leicht zu verwaltendes Netzwerk, um Anwendungen schnell und nahtlos bereitzustellen.

Avaya bietet diese Lösung mit der Avaya Virtual Enterprise Network Architecture (VENA) Unified Access.

Eine neue WLAN-Ära für Unternehmen

Für eine umfassende Mobilität im Unternehmen und für die Bewältigung des stark zunehmenden mobilen Datenverkehrs ist ein Umdenken hinsichtlich der derzeit eingesetzten WLAN-Architektur erforderlich.

Für viele Unternehmen bedeutet das Upgrade auf 802.11n und 802.11ac* den Beginn einer neuen WLAN-Ära, da diese Netze vor Einführung des Standards

*802.11ac ist ein in der Entwicklung befindlicher WLAN-Standard, der bis zum Ende des Jahres 2013 fertig gestellt werden sollte. Er ermöglicht einen WLAN-Durchsatz von mindestens 1 Gbit/s.

802.11n nur als sekundäres und ergänzendes Netzwerk für die verdrahtete Infrastruktur galten und im Allgemeinen ad hoc implementiert wurden, um die Ziele hinsichtlich Mobilität, Produktivität oder Kosteneinsparungen zu erreichen.

Der Standard 802.11n leitete eine neue Ära der WLAN ein, in der sie nicht mehr nur ein „Add-On-Netzwerk“ sind, sondern vielmehr ein integrierter Teil der IT-Unternehmensinfrastruktur, mit dem Mitarbeiter dauerhaften leistungsstarken, drahtlosen Zugang zu wichtigen Tools und Anwendungen erhalten. Dies umfasst auch die für Unternehmen besonders wichtige Unterstützung von bandbreitenintensiven Sprach- und Videoanwendungen in Echtzeit.

Um diese Anwendungsformen für Benutzer an allen Roaming-Standorten bereitstellen zu können, müssen die derzeitigen Ansätze für WLAN-Architekturen hinsichtlich der folgenden Aspekte neu überdacht werden:

- Skalierbarkeit: Herkömmliche WLAN-Architekturen bieten begrenzte Skalierbarkeit.
- Zuverlässigkeit: Die Zuverlässigkeit des WLAN muss sich mit der von verdrahteten LAN messen können.
- Quality of Service: WLAN müssen QoS für Mobilgeräte sicherstellen, indem der Netzwerkfluss priorisiert wird.
- Investitions- und Betriebsausgaben: Ausgaben für WLAN-Hardware und Verwaltungsressourcen müssen sinken.

Unzulänglichkeiten aktueller WLAN-Architekturen

Aktuelle WLAN-Architekturen, seien sie zentralisiert, verteilt oder eine Mischung der beiden Formen, weisen in verschiedenen Bereichen Mängel auf, darunter folgende:

Mangelnde Leistung: Viele bestehende WLAN-Architekturen wurden als Ergänzung konzipiert und niemals leistungsoptimiert. Sie waren auch nicht als primäre Netzwerkzugangsmethode gedacht. Daher gilt für bestehende WLAN-Architekturen Folgendes:

- Begrenzte Skalierbarkeit.
- Leistungsschwächen bei der integrierten Datenverkehrsverwaltung.
- LAN-Hardware als simple Verbindung, über die keine Optimierung der Hardware erfolgt.
- Keine Option für Echtzeitanwendungen.

Extra Hardwarekosten: Alle aktuellen Architekturansätze bezüglich WLAN erfordern eine maßgebliche Investition in zusätzliche Hardware, darunter folgende Extras:

- Geräte zum Steuern von Access Points.
- Server zum Verwalten des WLAN separat vom LAN.
- Geräte zum Sicherstellen der WLAN-Secutity.
- QoS-Funktionen.
- Separate Stromversorgungen zum Betreiben von Access Points in vielen Fällen.

Zuverlässigkeit: Alle aktuellen Ansätze leiden an Zuverlässigkeitsproblemen und weisen mehrere Fehlerstellen auf:

- Controller-Fehler wirken sich auf die Funktionalität der Steuerungs- und Datenebene aus.
- Es dauert normalerweise einige Minuten, bis das System nach einem Fehler wiederhergestellt wird, wobei Access Points im Allgemeinen neu gestartet werden und einen neuen Controller suchen müssen.
- Wenn sich mehr Komponenten in einem System befinden, müssen auch mehr Ersatzteile bereitgehalten werden. Zudem ist die Wahrscheinlichkeit größer, dass eine Komponente ausfällt.

WLAN-Management: Für alle Ansätze sind zusätzliche Managementressourcen erforderlich:

- Separate eigenständige Managementanwendung mit sehr begrenzter Integration in ein ganzheitliches Management-Framework.
- Eigenständige Managementanwendungen für Add-On-Lösungen, wie RFID-Tags, erweiterte WIDS-Sicherheit oder Gastzugänge.

Sicherheit: Alle Ansätze erfordern eine besondere Aufmerksamkeit hinsichtlich der Sicherheit:

- Funktionen wie Richtlinienumsetzung und Eindringungserkennung und -verhinderung (IDS/IPS) werden in eigenen Silos ausgeführt.
- WLAN-Produkte nutzen nur selten bereits vorhandene Security-Komponenten, wie Firewalls, IDS/IPS oder Endgeräte-Authentifizierung und verwenden in der Regel eigene Versionen dieser Funktionen. Damit wird das Management der Sicherheitsfunktionen noch komplizierter und anfälliger für Fehler bei Umsetzung von Richtlinien.

Es wird ein anderer Ansatz benötigt, eine Architektur der nächsten Generation, die die oben beschriebenen Probleme aufgreift und einen nahtlosen, überall verfügbaren und skalierbaren WLAN-Zugang ermöglicht. Die Lösung: Avaya VENA* Unified Access.

*Siehe seitliche Textleiste Avaya VENA

Ein neuer Ansatz: Avaya VENA Unified Access

Die Avaya VENA Unified Access-Lösung bietet Leistung, Skalierbarkeit und Flexibilität.

Der Versuch, einen Ausgleich zwischen Kosten, Leistung und Erreichbarkeit in den WLAN von heute zu erzielen, führt zu einer unaufhörlichen Reihe von Kompromissen. Keiner der aktuellen Architekturansätze bietet eine zufriedenstellende Lösung. Es wird eine Lösung benötigt, die die Fähigkeiten des zentralisierten Controllers nutzt, ohne die Leistung zu beeinträchtigen, und die dennoch eine Verteilung zulässt. Und genau das bietet Avaya VENA Unified Access.

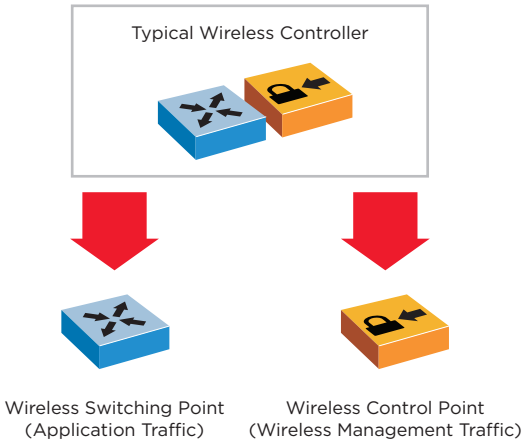

Abbildung 1: Wireless Controller

Was ist Unified Access?

Die Trennung der Datenebene (Transport der Nutzdaten) von der Verwaltungs- oder Steuerungsebene (auf der alle anderen Entscheidungen, einschließlich der Authentifizierung, getroffen werden) wurde schon in den ersten Controller-basierten Architekturen vollzogen. In vielen Fat-AP-Lösungen wurden Controller als ausschließliche Steuerungs- oder Sicherheits-/Firewall-Geräte implementiert, und die Datenebene wurde lokal auf dem Access Point (AP) belassen.

Avaya schlägt einen neuen Ansatz vor, bei dem die Kosten reduziert werden, da keine WLAN-Switching-Hardware benötigt wird. Anstatt sich darauf zu konzentrieren, ob die Datenebene am besten im Access Point oder im Controller verwaltet wird, wird die Wireless-Datenebene im Avaya-Ansatz, genannt Unified Access, direkt in das verdrahtete Netzwerk integriert und somit vollständig von den klassischen WLAN-Komponenten getrennt.

Der Unified Access-Ansatz von Avaya funktioniert folgendermaßen:

Herkömmliche Ethernet-Switches verfügen bereits über den Großteil der Funktionen, darunter auch die Prozessorleistung, die für eine systemeigene Bearbeitung des WLAN-Verkehrs erforderlich ist. Den herkömmlichen Ethernet-Switches fehlt jedoch der Mobilitätskontext für Roaming-Sitzungen, da ein Mobilgerät die IP-Adresse eines fremden Subnetzes überträgt, wenn es bewegt wird. Mithilfe eines Mobilitätsagenten, der dem Switch hinzugefügt wird, um Switching-Tabellen in Echtzeit beim Bewegen der Sitzungen zu programmieren, und mit etwas Unterstützung seitens der Steuerungsebene, werden beim Avaya Unified Access-Ansatz die IP-Adressinformationen aus fremden Subnetzen integriert. Und da durch das umfassende Einfügen von Software-Switching-Punkten oder durch das Rückholen von Paketen an einen anderen Standort, um Switching-Entscheidungen zu treffen, das WLAN nicht handlungsunfähig gemacht wird, ist der Avaya Unified Access-Ansatz effizienter, eleganter und effektiver als andere Ansätze.

Skalierbarkeit und Leistung: Da bestehende Controller nicht mehr durch Abläufe der Datenebene belastet werden, können sie ihre Steuerungsebenenkapazität um das Vielfache skalieren, indem Ressourcen erneut genutzt werden, die zuvor für das Datenebenen-Switching reserviert waren. Zu den zusätzlichen Vorteilen gehören die erhöhte Controller-Kapazität sowie das reduzierte Datenebenen-Tromboning, die Hardware-Tunnel-Verarbeitung sowie Overlay Traffic Forwarding-Hardware.

Zuverlässigkeit: Da die Datenebene die Zuverlässigkeitseigenschaften des zugrunde liegenden Ethernet-Switching-Netzwerks übernimmt, macht die WLAN-Zuverlässigkeit einen Riesensprung nach vorne. Jetzt da sich der WLAN-Controller außerhalb des Nutzdatenstroms befindet, können „single points of failure“ aus der WLAN-Datenebene entfernt werden. Die Funktionen für die Weiterleitung der Nutzdaten können aus dem herkömmlichen Controller ausgelagert werden. Das bedeutet, dass die 99,999%ige Zuverlässigkeit, die von dem klassenbesten Avaya Core-Netzwerk erzielt wird, automatisch von der WLAN-Lösung übernommen werden kann. Zudem wird die Steuerungsebene robuster, da der Ausfall eines Steuerungspunktes sich nicht direkt auf die Switching-Punkt-Funktionen auswirkt. Sitzungen arbeiten wie zuvor, selbst wenn ein einzelner Steuerungspunkt ausfällt, wodurch zum größten Teil die Notwendigkeit von komplexen, teuren aktiv/Standby- oder aktiv/aktiv-Failover-Funktionen entfällt.

Geringere Kosten und Virtualisierung der Steuerungsebene: Die Kosten werden minimiert, da die Notwendigkeit von teuren Controllern entfällt, um zig Gbit/s beim Datenverkehr-Switching bewältigen zu können. Zudem wird die Steuerungsebene, ohne besondere Switching-Hardware und bestimmte Port-Layouts zu benötigen, auf eine Reihe von Softwarefunktionen reduziert, die mühelos hinsichtlich der Skalierungsanforderungen pro Access

Vorteile einer Unified Wired/Wireless Architektur

Skalierbarkeit: Unabhängige Skalierung von Steuerungs- und Datenebenen gemäß den Anforderungen

Geringere Investitions- und Betriebskosten: Vereinheitlichung der Datenebene auf der Switching-Hardware und Virtualisierung der WLAN Kontrollebene führt zu weniger Geräten im Netz und zu einem geringeren Management- und Wartungsaufwand.

Größere Ausfallsicherheit: Die Avaya Unified Access-Lösung ermöglicht ein Clustering der Steuerungsebenen und bietet die Möglichkeit, die vorhandenen Hochverfügbarkeitslösungen des drahtgebundenen Netzwerks zu nutzen, z. B. Avaya VENA Switch Clustering.

Gemeinsame Richtlinie: Die zentralisierte Zugriffsrichtlinie von Avaya Identity Engines bietet eine konsistente Richtlinienumsetzung, Sicherheit und Gästeverwaltung. Zusammen mit Avaya VENA Unified Access stellt es eine umfassende Lösung für eine Unified Access-Ebene dar.

Verbesserte Leistung: Die Implementierung einer Avaya Unified Access-Lösung führt durch Soft- und Hardware-Synergien zu einer optimierten Plattform, die unter anderem die Weiterleitungslatenz und den Energieverbrauch reduziert.

Vereinfachung: Neben der Fähigkeit, die Datenebene als Unified Service auf einer gemeinsamen Switching-Hardware auszuführen, ermöglicht der Avaya Unified Access-Ansatz ein allgemeines Netzwerkmanagementsystem für Wireless-Funktionen und die Dateninfrastruktur.

Point quantifiziert werden können. Weiter wachsende Anforderungen hinsichtlich der Leistungsfähigkeit der Software können durch die ebenfalls wachsenden Fähigkeiten der Virtualisierungstechniken mit handelsüblichen Standardplattformen realisiert werden. Auf diese Weise werden die Controller-Kosten weiter reduziert, da die Steuerungsebene auf Virtualisierungsplattformen in modernen Rechenzentren vereinheitlicht wird. Hardwarekosten werden maßgeblich reduziert und durch eine kostengünstigere Softwarelizenzierungsstruktur ersetzt.

Unified Network Management: Im Avaya Unified Access-Ansatz wird aus der WLAN-Verwaltung eine Plug-in-Anwendung, die das gesamte Framework anderer Unified Management Anwendungen nutzt. Dank der Vereinheitlichung werden Betriebs- und Investitionskosten gesenkt.

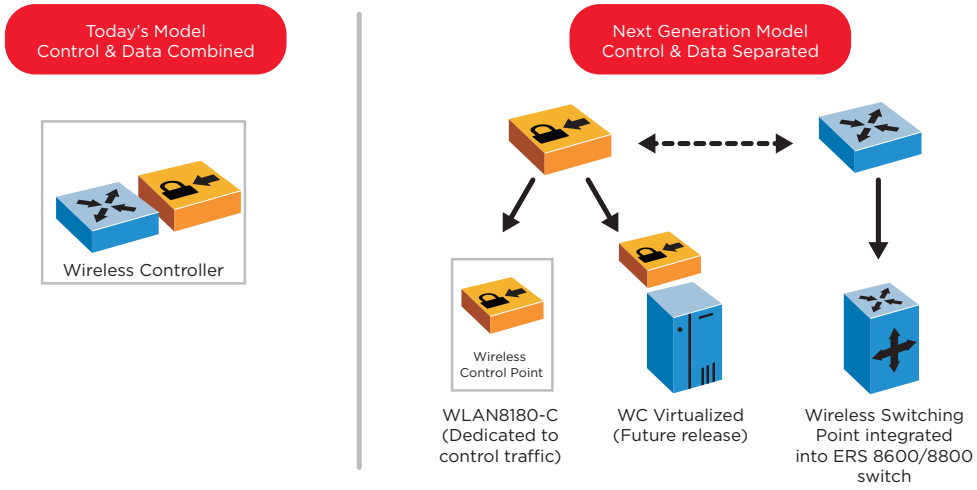

Abbildung 2: Altes Modell im Vergleich zum Avaya VENA Unified Access-Modell der nächsten Generation

Unified Identity und Network Access Control

Es ist wichtig, für jedes Gerät, jeden Nutzer und jede Anwendung bereits auf der Netzwerk Edge Ebene intelligente Authentifizierungsregeln bereit zu stellen. Auf diese Weise müssen Netzwerkadministratoren Benutzer oder Geräte nicht manuell einrichten und sich auch keine Gedanken darüber machen, ob Geräte Eigentum des Unternehmens oder eines Benutzers sind. Das Netzwerk erstellt ein Profil für (d. h. es identifiziert) ein BYOD-Gerät und stellt die Netzwerkkonnektivität basierend auf den geltenden Richtlinien automatisch her.

Avaya Identity Engines weist die Netzwerkzugriffsrechte und -berechtigungen basierend auf der Benutzerrolle, dem Benutzerstandort (lokal oder remote) und der Verbindungsart (verdrahtet oder drahtlos) zu. Je nach IT-Richtlinien

für Geräte kann der BYOD-Gerätezugriff auf bestimmte Ressourcen beschränkt werden, oder er kann als Gästegerät behandelt werden. Dank der Zentralisierung der Zugriffskontrolle wird der Zugriff auf verdrahtete und drahtlose Netzwerke vereinheitlicht. Systemadministratoren wird ein sehr einfacher und umfassender Einblick darauf gewährt, wer auf das Netzwerk zugegriffen hat und wer derzeit angemeldet ist.

Der Avaya Identity Engines Ignition Server führt die Benutzer- und Kontext-basierte Authentifizierung und Autorisierung für Clients durch, die auf das Netzwerk zugreifen möchten. Gebotene Unterstützung:

- AAA identitätsbasierte Netzwerkzugriffskontrolle
- Eine leicht zu verwendende, standardbasierte Richtlinien-Engine
- RADIUS-Integration mit allen Unternehmensnetzwerkgeräten
- Schnelle und umfassende Integration in wichtige Verzeichnisse

Avaya VENA Unified Access – Integrieren von Avaya WLAN 8100 und dem Avaya Ethernet Routing Switch 8800

Avaya WLAN 8100

Als WLAN-Lösung der nächsten Generation ist Avaya WLAN 8100 darauf ausgelegt, eine skalierbare Basis mit sehr hoher Performance zu bieten, die es Unternehmen ermöglicht, die Vorteile mobiler Kommunikation im Unternehmen maximal auschöpfen zu können. Die Avaya WLAN 8100-Serie besteht aus drei Kernelementen:

- **WLAN-Access Points** ermöglichen den drahtlosen Netzwerkzugriff durch mobile Geräte. Sie ver- und entschlüsseln den drahtlosen Datenverkehr und überwachen die Funkfrequenzen zur Identifizierung und Eindämmung von nicht autorisierten Access Points.
- **WLAN-Controller,** steuern die Access Points und stellen wichtige Funktionen im Bereich Sicherheit, Netzwerk, Quality of Service (QoS) und Roaming für mobile Benutzer zur Verfügung. Controller können als eigenständige Wireless-Controller (Steuerungs- und Datenverkehr) oder als zugewiesene Steuerungspunkte bereitgestellt werden, wobei die Datenebene als Teil der VENA Unified Access Architecture in die Ethernet Routing Switches ERS 8800 integriert ist.
- **Die WLAN Management Software** ist ein umfassendes Design- und Management-Tool, mit dem die ideale Position von Access Points auf Grundrissen identifiziert wird. Sie konfiguriert alle Geräte mit einem einzelnen Klick und ermöglicht eine präzise Überwachung und Berichterstattung für umfassende Transparenz und Steuerung des gesamten Systems.

Avaya ERS 8800

Der Ethernet Routing Switch 8800 ist eine Kollektion modularer Ethernet-Switching-Systeme, die dauerhaft aktive Netzwerkverbindungen und hohe Konnektivität dank hoher Portdichte bieten. Er unterstützt Hot-Swap-Module, redundante Lüfter sowie Netzteile. Jede dieser einzelnen Plattformen ist für besonders hohe Ausfallsicherheit konzipiert und bietet in Switch-Cluster-Konfigurationen eine besonders hohe Verfügbarkeit und somit dauerhaften Zugriff auf Anwendungen. Verfügbar in einer Vielzahl unterschiedlicher Modelle wurden diese Systeme speziell unter Berücksichtigung der wichtigen Unternehmensanforderungen hinsichtlich Ausfallsicherheit, Effizienz und Skalierbarkeit entwickelt.

Der Ethernet Routing Switch 8800 ist eine Hauptkomponente der Avaya Virtual Enterprise Network Architecture, die den vollen Funktionsumfang der Netzwerkvirtualisierung für Unternehmens- und Rechenzentrumsanwendungen unterstützt.

Avaya Virtual Enterprise Network Architecture (VENA)

Die Avaya Virtual Enterprise Network Architecture (VENA) ist ein immer verfügbares unternehmensweites Virtualisierungs-Framework, das das Netzwerk vereinfacht und die Bereitstellung von Cloud-basierten Services optimiert. Es bietet Unternehmen die Möglichkeit, erfolgreich Architekturen der nächsten Generation, z. B. die private Cloud, zu erstellen und zu betreiben.

Avaya VENA fasst verschiedene sich ergänzende, bedeutende Funktionen zusammen – davon sind einige bereits länger etabliert und andere sind neu –, sodass sie eindeutig als strategische, zweckmäßige und unternehmensorientierte Lösungen identifiziert werden. Das Wichtigste ist es daher zu wissen, dass alle Komponenten, unabhängig davon, ob es sich um ein vorhandenes Avaya VENA Switch Clustering oder um den neuen Avaya VENA Unified Access handelt, als Teil der Avaya VENA-Strategie speziell auf hohe Verfügbarkeit, Leistung und geringe Komplexität ausgelegt sind.

Avaya VENA-Lösungen wurden konzipiert, um die Anforderungen von Unternehmen zu erfüllen, die im harten internationalen Wettbewerb stehen. Durch das Abstimmen der Unternehmensziele mit den Anforderungen an das Unternehmensnetzwerk werden die VENA-Lösungen so konzipiert, dass sie eine wesentlich geringere Komplexität, längere Betriebslaufzeiten sowie einen höheren Datendurchsatz als herkömmliche Netzwerk-architekturen bieten.

Das Identity Engines Ignition Access Portal gewährt Benutzern Zugriff, die Geräte verwenden, die das 802.1x-Protokoll nicht unterstützen. Darüber hinaus auch Benutzern mit nicht verwalteten Geräten. Des Weiteren kann das Access Portal den Identity Engines Ignition CASE Client hosten, der die automatische Konfiguration von verwalteten und nicht verwalteten Geräten für einen drahtgebundenen und drahtlosen sicheren Zugriff aktiviert.

Avaya Identity Engines unterstützt auch das Unified Guest Access Management. Mit dem Avaya Identity Engines Guest Manager können Frontdesk-Mitarbeiter eindeutige Benutzer-IDs und Kennwörter für jeden Besucher erstellen, um sichere und bequeme Netzwerkverbindungen für Gäste und temporäre Benutzer zu bieten. Mitarbeiter und auch Gäste können den Zugriff selbst bereitstellen.

Ein wichtiger Nutzen der Avaya Identity Engines-Lösung für den Gästezugriff besteht darin, eine einheitliche Lösung zu bieten. Ein Benutzer erhält einmaligen Zugriff und, je nachdem, ob er die Verbindung drahtgebunden oder drahtlos herstellt, wird er demselben Sicherheitsprofil zugewiesen.

Fazit: Ein skalierbares, leistungsstarkes Unified Network

Avaya stellt eine einheitliche Zugriffslösung bereit, die die wichtigsten, aktuellen Herausforderungen für Unternehmen berücksichtigt.

Die Avaya Unified Access-Lösung bietet überall Zugriff auf Unternehmensanwendungen und Unified Communications-Tools, die sich positiv auf die Produktivität und Leistung des Unternehmens auswirken können. Durch die Integration der Wireless-Datenebene in das verdrahtete Datennetzwerk mittels eines Unified Access-Ansatzes beseitigt diese Lösung die Nachteile der aktuellen zentralisierten und verteilten WLAN-Ansätze und kreiert eine skalierbare, zuverlässige und leistungsstarke Architektur für die mobile Zukunft.

Die Avaya Unified Access- und Identity Engines-Services sind bereits heute verfügbar, um ein intelligentes Netzwerk Edge betreiben zu können. Damit werden die Kosten durch technische Synergieeffekte reduziert. Die sichere Authentifizierung und automatische Bereitstellung von Netzwerkzugriffen erfolgt ohne wiederholte Eingriffe eines Netzwerkadministrators.

Über Avaya

Avaya ist ein weltweiter Anbieter von Kommunikationssystemen für Unternehmen jeder Größenordnung. Dazu gehören Lösungen für Unified Communications, Contact Center und Netzwerke sowie Dienstleistungen. Weitere Informationen finden Sie auf **www.avaya.de**.

02/13 • DN7118GE